**Deutscher Bundestag** **Drucksache 17/9640**

**17. Wahlperiode** 15. 05. 2012

# Antwort

## der Bundesregierung

### auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE.
### – Drucksache 17/9305 –

### „Strategische Fernmeldeaufklärung“ durch Geheimdienste des Bundes

Vorbemerkung der Fragesteller

Das Bundesamt für Verfassungsschutz (BfV), der Bundesnachrichtendienst (BND) und der Militärische Abschirmdienst (MAD) dürfen den elektronischen Datenverkehr unter anderem im Rahmen der Terrorabwehr durchforsten. Ähnliches gilt für das Zollkriminalamt (ZKA), das auch entsprechende nachrichtendienstliche Befugnisse hat. Am 25. Februar 2012 berichtete die „Bild“-Zeitung unter Berufung auf zwei Berichte des Parlamentarischen Kontrollgremiums (PKGr) des Deutschen Bundestages, dass im Jahr 2010 mehr als 37 Millionen E-Mails und Datenverbindungen von den deutschen Geheimdiensten überprüft wurden, weil darin bestimmte Schlagwörter wie „Bombe“ vorkamen. Damit hätte sich die Zahl im Vergleich zum Vorjahr mehr als verfünffacht. Nach PKGr-Angaben ergaben die Überwachungsmaßnahmen insgesamt nur in 213 Fällen verwertbare Hinweise für die Geheimdienste.

Das PKGr schreibt in seinem Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 dieses Gesetzes (Bundestagsdrucksache 17/8639), dass 2010 die Behörden in E-Mails und anderen Kommunikationen nach rund 16 400 Begriffen gesucht hätten. Der größte Teil (rund 13 000) entfiel dabei auf den Bereich des Waffenhandels; dort wurden auch mit 25 Millionen die meisten Gespräche und Mail-Konversationen erfasst. Davon wurden letztlich jedoch nur 180 als „nachrichtendienstlich relevant“ eingestuft; „hierbei handelte es sich um 12 E-Mail-, 94 Fax- und 74 Sprachverkehre“, heißt es in dem Bericht. Das PKGr führt das Verhältnis zwischen Aufwand und Erfolg unter anderem auf das Spam-Aufkommen zurück: „Die zur Selektion unerlässliche Verwendung von inhaltlichen Suchbegriffen, bei denen es sich auch um gängige und mit dem aktuellen Zeitgeschehen einhergehende Begriffe handeln kann, führt unweigerlich zu einem relativ hohen Spam-Anteil, da viele Spam-Mails solche Begriffe ebenfalls beinhalten können“. Es liegt nahe, dass Wörter, Satzteile oder Phoneme gleicher Bedeutung parallel in mehr als einer Sprache verwendet werden.

*Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundeskanzleramtes vom 11. Mai 2012 übermittelt.*
*Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.*

Nach Angaben von PKGr-Mitgliedern handle es sich bei der Maßnahme nicht um eine Rasterfahndung im Telekommunikationsverkehr bestimmter deutscher Bürger in Deutschland, sondern um eine „strategische Überwachung der gebündelten Funkübertragung etwa über asiatischen oder afrikanischen Ländern“. Deutsche dürften hiervon kaum betroffen sein. Falls doch, gelte für sie prinzipiell der Schutz des Grundgesetzes mit der Pflicht zur sofortigen Datenlöschung. Über die Zulässigkeit und Notwendigkeit der Anordnung einschließlich der Verwendung von Suchbegriffen entschieden die im PKGr vertretenen unabhängigen Fachleute (vgl. heise.de vom 27. Februar 2012).

Das PKGr schreibt in seinem Bericht: „Strategische Kontrolle bedeutet, dass nicht der Post- und Fernmeldeverkehr einer bestimmten Person, sondern Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt, nach Maßgabe einer Quote insgesamt überwacht werden. Aus einer großen Menge verschiedenster Gesprächsverbindungen werden mit Hilfe von Suchbegriffen einzelne erfasst und ausgewertet“. Nach Ansicht der Fragesteller und Angaben von Experten müssen die Geheimdienste jedoch, wenn sie bestimmte Suchbegriffe in E-Mails finden wollen, jede E-Mail filtern. Technisch bedient man sich hierbei einer „Parsing“ genannten Syntaxanalyse.

## Vorbemerkung der Bundesregierung

„Strategische Fernmeldeaufklärung“ dient der Aufklärung einzelner Gefahrenbereiche, indem unter bestimmten Voraussetzungen gebündelt übertragene internationale Telekommunikationsverkehre erfasst werden können. Nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G10) ist dieser Aufklärungsansatz ausschließlich dem Bundesnachrichtendienst (BND) vorbehalten (vgl. Abschnitt 3 G10). Sämtliche Antworten, ausgenommen diejenigen zu den Fragen 9c, 9d, 15 und 17, beziehen sich demnach ausschließlich auf die strategische Fernmeldeaufklärung des BND im Geltungsbereich des G10.

1. Inwieweit werden neben Internetverkehr, E-Mails, Faxverbindungen, Webforen und Sprachverkehren durch deutsche Geheimdienste weitere Kommunikationskanäle im Rahmen der „strategischen Fernmeldeaufklärung“ ausgespäht?

   a) Auf welche Art und Weise wurden die „12 E-Mail-, 94 Fax- und 74 Sprachverkehre“ im Bereich „Proliferation und konventionelle Rüstung“ sowie die „7 Metadatenerfassungen, 17 Webforenerfassungen und 5 Sprachverkehre“ im Bereich „Internationaler Terrorismus“ erhoben (Bundestagsdrucksache 17/8639)?

   b) Was ist mit der „Metadatenerfassung“ gemeint, und auf welche Art und Weise wird diese vorgenommen?

Einzelheiten zu den technischen Fähigkeiten des BND können in diesem Zusammenhang nicht öffentlich dargestellt werden, da aus ihrem Bekanntwerden sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf den Modus Operandi, die Fähigkeiten und Methoden der Behörde ziehen und so eine Erfassung vermeiden könnten. Bei der Beantwortung findet u. a. entsprechendes operatives Vorgehen Erwähnung. Im Ergebnis könnte dies für die Funktionsfähigkeit der Sicherheitsbehörde und mithin für die Interessen der Bundesrepublik Deutschland schädlich sein oder aber die Sicherheit der Bundesrepublik Deutschland gefährden. Gleichwohl wird die Bundesregierung nach gründlicher Abwägung dem Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen nachkommen.

Die Informationen werden als „Geheim“ und „VS – Vertraulich“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

c) Welche weiteren sechs Kommunikationsverkehre wurden im „Gefahrenbereich ‚Illegale Schleusung‘“ neben ausspionierten E-Mails erfasst?

Im Jahr 2010 wurden für den Gefahrenbereich Illegale Schleusung neben E-Mails Sprachverkehre erfasst.

2. Nach welchem technischen Verfahren werden die Kommunikationsverkehre durchforstet?

a) Trifft es zu, dass der BND, der MAD und das BfV sowie das ZKA hierfür Software der Firmen trovicor GmbH, Utimaco AG, Ipoque GmbH oder ATIS UHER einsetzen, und falls ja, um welche konkreten Anwendungen handelt es sich?

b) Wenn nicht, von welchen Firmen oder welcher Firma stammt die eingesetzte Software?

c) Handelt es sich dabei um ein Parsing, Tagging, einen Stringvergleich oder andere Verfahren der Zuordnung von Wortklassen?

d) Wie viele Mitarbeiter sind jeweils mit der Durchführung dieser Maßnahme betraut?

Einzelheiten zu den technischen Fähigkeiten des BND sowie der Zahl der eingesetzten Mitarbeiter können in diesem Zusammenhang nicht öffentlich dargestellt werden, da aus ihrem Bekanntwerden sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf den Modus Operandi, die Fähigkeiten und Methoden der Behörde ziehen könnten. Bei der Beantwortung der hiesigen Frage wird auf entsprechende Fähigkeiten, Methoden sowie auf Kapazitäten der strategischen Fernmeldeaufklärung eingegangen. Es steht zu befürchten, dass eine offene Beantwortung entsprechenden Akteuren die Möglichkeit eröffnen würde, eine Erfassung zu vermeiden. Im Ergebnis könnte dies für die Funktionsfähigkeit der Sicherheitsbehörde und mithin für die Interessen der Bundesrepublik Deutschland schädlich sein. Gleichwohl wird die Bundesregierung nach gründlicher Abwägung dem Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen nachkommen.

Die Informationen werden als „VS – Vertraulich“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

3. Ist die eingesetzte Technik auch in der Lage, verschlüsselte Kommunikation (etwa per Secure Shell oder Pretty Good Privacy) zumindest teilweise zu entschlüsseln und/oder auszuwerten?

Ja, die eingesetzte Technik ist grundsätzlich hierzu in der Lage, je nach Art und Qualität der Verschlüsselung.

---

* Das Bundeskanzleramt hat die Antwort als „VS – Vertraulich“ und „VS – Geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

4. Wie hoch sind die Kosten für die Kommunikationsüberwachung im Rahmen der „strategischen Fernmeldeaufklärung“, aufgelistet nach
   - den Kosten für die Anschaffung der technischen Ausrüstung,
   - den laufenden Kosten für die technische Ausrüstung,
   - den Personalkosten und
   - den sonstigen Kosten?

Eine Auflistung der konkreten Kosten für die Kommunikationsüberwachung im Rahmen der strategischen Fernmeldeaufklärung kann Rückschlüsse auf die technischen Fähigkeiten sowie auf das Aufklärungspotential des BND zulassen. Aus diesem Grund muss ausnahmsweise der parlamentarische Auskunftsanspruch vor dem Geheimhaltungsinteresse des BND insoweit zurücktreten als die nachstehende Antwort mit einem Verschlusssachengrad „Geheim“ eingestuft und zur Auslage in der Geheimschutzstelle des Deutschen Bundestages bestimmt wird.*

5. Auf welche Art und Weise werden die „Stichproben“ der „strategischen Fernmeldeaufklärung“ bestimmt?
   a) Was ist mit der „Maßgabe einer Quote“ gemeint, nach der „Gesprächsverbindungen“ – laut Bundestagsdrucksache 17/8639 – ausgespäht werden?
   b) Nach welchen Kriterien werden die Rasterungen gemäß dieser „Quote“ vorgenommen?

Der Bundesregierung ist im Rahmen der strategischen Fernmeldeaufklärung der Begriff „Stichproben“ nicht bekannt. Der auf Bundestagsdrucksache 17/8639 verwendete Begriff der „Quote“ bezieht sich auf die in § 10 Absatz 4 Satz 3 und 4 G10 gesetzlich vorgegebene Kapazitätsbegrenzung. Danach darf in den Fällen strategischer Beschränkungen nach § 5 G10 höchstens 20 Prozent der auf den angeordneten Übertragungswegen insgesamt zur Verfügung stehenden Übertragungskapazität überwacht werden. Hierzu fordert der BND gemäß § 2 Absatz 1 Satz 3 G10 infrage kommende Telekommunikationsdienstleister auf, an Übergabepunkten gemäß § 27 der Telekommunikations-Überwachungsverordnung (TKÜV) eine vollständige Kopie der Telekommunikationen bereitzustellen, die in den angeordneten Übertragungswegen vermittelt wird. Innerhalb dieser Quote werden durch Abfolge festgelegter Bearbeitungsschritte und anhand der ebenfalls antragsgemäß angeordneten Suchbegriffsprofile bzw. Filterkriterien meldungswürdige Ergebnisse aus dem erfassten Kommunikationsaufkommen selektiert.

6. Wie wurden die 16 400 Begriffe, nach denen die Kommunikation durchforstet wird, bestimmt?
   a) Welche Abteilung ist hierfür jeweils zuständig?

Die zur Beantragung vorgeschlagenen Suchbegriffe werden durch die zuständigen auswertenden Abteilungen LA, LB, TE und TW des BND anhand am Aufklärungsprofil orientierter, fachlicher und technischer Erwägungen unter Berücksichtigung der gesetzlichen Vorgaben festgestellt. Die Anordnung erfolgt

* Das Bundeskanzleramt hat die Antwort als „VS – Geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

durch das Bundesministerium des Innern nach Maßgabe der §§ 9, 10 G10 mit Zustimmung der G10-Kommission, § 15 Absatz 5, 6 G10.

b) Auf welche weiteren Analysen welcher weiteren Behörden oder Institutionen wird dabei zurückgegriffen?

Einzelheiten zur Frage können in diesem Zusammenhang nicht öffentlich dargestellt werden, da aus ihrem Bekanntwerden sowohl staatliche als auch nichtstaatliche Akteure wiederum Rückschlüsse auf den Modus Operandi, die Fähigkeiten, Methoden und hier auch zu möglichen Kooperationsverhältnissen der Behörden ziehen könnten. Im Ergebnis könnte dies für die Funktionsfähigkeit der Sicherheitsbehörden und mithin für die Interessen der Bundesrepublik Deutschland schädlich sein. Gleichwohl wird die Bundesregierung nach gründlicher Abwägung dem Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen nachkommen.

Die Informationen werden als „VS – Vertraulich“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

7. Wie viele TK-Verkehre (TK = Telekommunikation) werden bzw. wurden tatsächlich gefiltert, um auf die angegebenen Zahlen zu kommen (bitte nach E-Mails, Fax- und Sprachverkehren aufschlüsseln)?

   Sofern keine Angabe zur konkreten Zahl möglich sein soll, in welcher Größenordnung bewegt sich die Zahl?

Der Anteil der mittels Suchbegriffen auf den angeordneten Übertragungswegen zu überwachenden Übertragungskapazität (§ 10 Absatz 4 Satz 3 G10) liegt als Rohdatenstrom vor, nicht aber in Form einzelner Verkehre. Aus diesem qualifizierten sich im Jahr 2010 ca. 37 Millionen E-Mails anhand der Suchbegriffe. Diese wurden einer anschließenden SPAM-Filterung zugeführt. Die Größenordnung variiert abhängig von übertragungstechnischen Gegebenheiten und jeweils angeordnetem Suchbegriffsprofil. Bei den erfassten E-Mail-Verkehren lag der Anteil an SPAM bei etwa 90 Prozent.

Einzelheiten im Übrigen können in diesem Zusammenhang nicht öffentlich dargestellt werden. Aus ihrem Bekanntwerden könnten sowohl staatliche als auch nichtstaatliche Akteure wiederum Rückschlüsse auf die Fähigkeiten und Methoden der Behörde ziehen. Im Ergebnis würde dadurch die Funktionsfähigkeit der Sicherheitsbehörde und mithin die Sicherheit der Bundesrepublik Deutschland beeinträchtigt. Gleichwohl wird die Bundesregierung nach gründlicher Abwägung dem Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen nachkommen.

Die Informationen werden als „Geheim“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

8. Wurden die tatsächlich gefilterten und/oder erfassten TK-Verkehre protokolliert?

Die Durchführung der strategischen Fernmeldeaufklärung wird gemäß § 5 Absatz 2 Satz 4 G10 protokolliert.

---

* Das Bundeskanzleramt hat die Antwort als „VS – Vertraulich“ und „VS – Geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

a) Wenn ja, wer ist berechtigt, diese Protokolle auszuwerten, und zu welchem Zweck?

Gemäß § 5 Absatz 2 Satz 5 G10 dürfen die Protokolldaten ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. Sie stehen daher den gesetzlich befugten Funktionsbereichen der behördlichen Datenschutzkontrolle und insbesondere der G10-Kommission, sowie dem auch insoweit umfassend zuständigen Kontrollgremium zur Verfügung, § 15 Absatz 5 Satz 2 G10, §§ 14 Absatz 1 G10, 5 Absatz 1 des Kontrollgremiumgesetzes – PKGrG.

b) Welche Informationen werden protokolliert?

Es werden alle Zugriffe und Arbeitsschritte protokolliert.

9. Werden bei der „strategischen Fernmeldeaufklärung“ Kommunikationsverkehre lediglich von und nach Deutschland ausgespäht?

Im Geltungsbereich des G10 werden ausschließlich Telekommunikationsverkehre von und nach Deutschland erfasst. Darüber hinaus führt der BND Fernmeldeaufklärung im Ausland durch. Insoweit wird auch auf die Antwort zu Frage 15 hingewiesen.

a) Falls nein, wie viele der überwachten Kommunikationsverkehre bezogen sich auf Verbindungen ins Ausland?

Auf die Antworten zu den Fragen 9 und 9b wird verwiesen.

b) Falls ja, wie wird bei der strategischen Auswertung von E-Mails zwischen rein inländischen und Verkehren aus dem und in das Ausland unterschieden, insbesondere dann, wenn der E-Mail- oder Webblog-Provider keine „.de“-Adresse verwendet bzw. der Server im Ausland steht?

Die Antwort auf die Frage kann nicht öffentlich dargestellt werden. Sie beschreibt Fähigkeiten, insbesondere aber auch Methoden und Verfahren der strategischen Fernmeldeaufklärung bei der Erfassung von E-Mails. Eine Offenlegung würde staatlichen und nichtstaatlichen Akteuren, beispielsweise Gefährdern, Hinweise auf Verdeckungsmöglichkeiten geben, die die Funktion der strategischen Fernmeldeaufklärung in diesem Sektor erheblich einschränken und eine Gefahr für die Auftragserfüllung des BND und somit auch für die Sicherheit der Bundesrepublik Deutschland darstellen könnten. Gleichwohl wird die Bundesregierung nach gründlicher Abwägung dem Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen nachkommen.

Die Informationen werden als „Geheim“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

c) Was versteht die Bundesregierung unter „Webblog-Kommunikation“?

Die Bundesregierung versteht unter Webblog ein öffentliches Forum, dessen Inhalte nicht als Individualkommunikation zu qualifizieren sind.

* Das Bundeskanzleramt hat die Antwort als „VS – Geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

d) Inwieweit wird bei der „Webblog-Kommunikation“ bestimmt, ob es sich dabei nicht um eine „innerdeutsche“ Kommunikation handelt?

Eine Differenzierung zwischen „innerdeutscher“ und anderer Kommunikation erübrigt sich. Auf die Antwort zu Frage 9c wird insoweit verwiesen.

e) Inwieweit werden Kommunikationsverkehre auch nach den Adressen bzw. Telefonnummern der Absender (Absenderkennung) oder Adressaten (Zielkennung) gefiltert?

Die Filterung und Selektion des BND zu Zwecken der strategischen Fernmeldeaufklärung richtet sich primär nach objektiven und gegebenenfalls konkret zuordenbaren Telekommunikationsmerkmalen gemäß § 5 Absatz 2 G10.

10. Inwieweit wird unterschieden, ob ein Kommunikationsverkehr für die weitere Beobachtung oder Strafverfolgung relevant ist?

In einem mehrstufigen Bewertungsverfahren wird nach Abschluss des automatisierten Selektions- und Filterungsprozesses durch die fachlich zuständigen Auswerter die Relevanz der Kommunikationsverkehre geprüft. Anschließend wird gesondert geprüft, ob eine Übermittlung gemäß §§ 7, 7a, 8 G10 in Betracht kommt.

a) Werden auch firmeninterne Kommunikationsverkehre überwacht, indem etwa E-Mails zwischen gleichen Domains ausgespäht werden?

Im Rahmen der strategischen Fernmeldeaufklärung, die nur auf angeordneten Übertragungswegen ansetzt, gelten für firmeninterne Kommunikationsverkehre keine gesonderten Regelungen, § 10 Absatz 4 Satz 2 G10.

b) Inwieweit wird sichergestellt, dass Abgeordnete, Rechtsanwältinnen/ Rechtsanwälte, Journalistinnen/Journalisten oder Diplomaten von den Spionagemaßnahmen ausgeschlossen werden?

Sofern im Rahmen der strategischen Fernmeldeaufklärung nach Abschnitt 3 G10 Anhaltspunkte dafür bestehen, dass Angehörige des entsprechend geschützten Personenkreises als Teilnehmer erfasst werden, wird durch zusätzliche Recherchemaßnahmen abgeklärt, ob ein materiell vergleichbarer Fall zu § 3b G10 vorliegt und die Erfassung gegebenenfalls rückstandslos gelöscht.

11. Auf welche Art und Weise und wie lange wurden bzw. werden die Kommunikationsverkehre für die Auswertung gespeichert oder kurzzeitig vorgehalten?

Der Anteil der mittels Suchbegriffen auf den angeordneten Übertragungswegen zu überwachenden Übertragungskapazität (§ 10 Absatz 4 Satz 3 G10) wird als Datenmenge nicht gespeichert. Eine Speicherung erfolgt erst nach dem Suchdurchlauf.

a) Auf welche Art und Weise werden gefundene „Treffer“ weiter bearbeitet?

Als Treffer werden G10-Nachrichten mit angeordnetem Suchbegriff verstanden. Ist ein angeordneter Suchbegriff in einer Kommunikation enthalten, wird die entsprechende Nachricht durch den hierzu besonders ermächtigten Bearbeiter erstmals auf nachrichtendienstliche Relevanz geprüft. Bei festgestellter Re-

levanz wird die Meldung einer nochmaligen Überprüfung sowie einer zweiten Relevanzprüfung durch den fachlich zuständigen Auswertebereich zugeführt. Es werden nur Treffer bearbeitet.

b) Wo werden vermeintliche „Treffer“, also Kommunikationsverkehre mit „verdächtigem“ Vokabular weiter gespeichert, und wer hat darauf Zugriff?

c) Wie lange bleiben die TK-Verkehre bei diesem Prozess (ggf. auch nur in einem temporären Speicher) gespeichert (bitte nach E-Mails, Fax- und Sprachverkehren aufschlüsseln)?

Einzelheiten zu den Fragen können in diesem Zusammenhang nicht öffentlich dargestellt werden, da aus ihrem Bekanntwerden sowohl staatliche als auch nichtstaatliche Akteure wiederum Rückschlüsse auf Verfahren, Methoden und Fähigkeiten der Behörde ziehen und Verdeckungsmöglichkeiten ableiten könnten. Im Ergebnis könnte dies für die Funktionsfähigkeit der Sicherheitsbehörde und mithin für die Interessen der Bundesrepublik Deutschland schädlich sein. Gleichwohl wird die Bundesregierung nach gründlicher Abwägung dem Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen nachkommen.

Die Informationen werden als „VS – Vertraulich“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

d) Wie ist der Umgang mit nicht relevanten, aber erfassten TK-Daten?

Sofern keine Relevanz festgestellt wird, erfolgt eine unverzügliche und rückstandslose Löschung.

e) Wie viele der erfassten TK-Verkehre waren unbrauchbar auf Grund von „Spam“?

Im Jahr 2010 lag der Anteil an SPAM bei den erfassten E-Mail-Verkehren bei etwa 90 Prozent.

12. Inwieweit werden Kommunikationsverkehre auch durch die Auswertung gesprochener Wörter ausgespäht?

Teile der Antwort zu Frage 12 können in diesem Zusammenhang nicht öffentlich dargestellt werden, da aus ihrem Bekanntwerden sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf den Modus Operandi, die Fähigkeiten und Methoden der Behörde ziehen und ihr Verhalten entsprechend ausrichten könnten. Im Ergebnis würde dadurch die Funktionsfähigkeit der Sicherheitsbehörde und mithin die Sicherheit der Bundesrepublik Deutschland beeinträchtigt. Gleichwohl wird die Bundesregierung nach gründlicher Abwägung dem Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen nachkommen.

Die Informationen werden als „Geheim“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

* Das Bundeskanzleramt hat die Antwort als „VS – Vertraulich“ und „VS – Geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

a) Werden Wörter bzw. Satzteile oder Phoneme gleicher Bedeutung parallel in mehr als einer Sprache als Suchbegriff verwendet?

Auf die Antwort zu Frage 12 wird verwiesen.

b) Welche Abteilungen bei BND, MAD und BfV sind zuständig für die Entwicklung von Systemen zur Spracherkennung?

Die Abteilung TK des BND wäre zuständig.

13. Worauf stützt die Bundesregierung die Behauptung, der Anstieg der überwachten Kommunikationsverkehre sei dem steigenden Versand von Spam-E-Mails geschuldet, obschon dieser im fraglichen Zeitraum laut anderen Statistiken eher zurückgegangen war?

Die Aussage ergibt sich aus den tatsächlichen Ergebnissen der strategischen Fernmeldeaufklärung.

14. In wie vielen Fällen waren die erlangten „Erkenntnisse“ ermittlungsrelevant oder trugen wesentlich zur Aufklärung oder Abwehr schwerer Straftaten bei?

a) Sofern hierzu keine Statistiken mitgeteilt werden können, in welcher Größenordnung bewegen sich etwaige „positive“ Ergebnisse?

b) Wie verteilten sich die gefundenen Treffer auf die Kriminalitätsphänomene „Bewaffneter Angriff auf die Bundesrepublik Deutschland“, „Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland“, „Internationale Verbreitung von Kriegswaffen“, „Unbefugte gewerbs- oder bandenmäßig organisierte Verbringung von Betäubungsmitteln“, „Beeinträchtigung der Geldwertstabilität im Euro-Währungsraum durch im Ausland begangene Geldfälschungen“, „International organisierte Geldwäsche“, „Gewerbsmäßig oder bandenmäßig organisiertes Einschleusen von ausländischen Personen?

Es gibt Fälle, in denen die erlangten „Erkenntnisse“ sich nach Übermittlung gemäß § 7 Absatz 4 G10 als ermittlungsrelevant erwiesen haben oder wesentlich zur Aufklärung oder Abwehr schwerer Straftaten beigetragen haben. Statistiken sind hierzu nicht vorhanden.

Hinzuweisen ist in diesem Zusammenhang auf die grundsätzlich anders geartete Zielrichtung von Maßnahmen der strategischen Fernmeldeaufklärung und Mitteln der Erkenntnisgewinnung im Strafverfahren. Zweck der strategischen Fernmeldeaufklärung ist die Auslandsaufklärung im Hinblick auf bestimmte außen- und sicherheitspolitisch relevante Gefahrenlagen (BVerfG, NJW 2000, S. 55 ff., 63). Dem nachrichtendienstlichen Trennungsgebot entsprechend zielt sie nicht auf die Ermittlung eines konkreten Sachverhalts innerhalb des Gefüges der Verfahrensregeln des Strafprozessrechts. Die Übermittlungsvorschriften der §§ 7, 7a und 8 Absatz 6 G10 sind Ausdruck dieses Trennungsgebots sowie Beleg der mangelnden Eignung strafprozessualer Statistiken zur Feststellung der Sinnhaftigkeit der gefahrenbereichsbezogenen Vorschriften des § 5 ff. G10.

15. Durch welche weiteren Maßnahmen nehmen BND, MAD und BfV ihre gesetzlichen Aufgaben zur Überwachung des Telekommunikationsverkehrs wahr?

Das BfV, der MAD und der BND können entsprechend dem Abschnitt 2 G10 nur in Einzelfällen Beschränkungen zur Telekommunikationsüberwachung beantragen. Daneben können auch Maßnahmen nach § 8a des Bundesverfassungsschutzgesetzes – BVerfSchG (gegebenenfalls in Verbindung mit § 4 MAD-Gesetz und § 2a BND-Gesetz) zur Erlangung von Telekommunikationsverkehrsdaten (keine Inhaltsdaten) im Einzelfall beantragt werden.

Der BND ist gemäß § 1 Absatz 2 Satz 1 BND-Gesetz mit der Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung sind, beauftragt. Hierzu setzt er auch das Mittel der strategischen Fernmeldeaufklärung im Ausland sowie informationstechnische Operationen ein.

16. An welchem Ort stehen die vom BND genutzten Informationssysteme bzw. die zur „strategischen Fernmeldeaufklärung“ genutzte Hardware?

    a) Inwieweit greifen Bundesbehörden zur Überwachung von Telekommunikation auf den Verkehr über den Frankfurter Netzknoten DE-CIX (German Commercial Internet Exchange) zu?

    b) Inwieweit arbeiten Bundesbehörden zur „strategischen Fernmeldeaufklärung“ auch mit den kommerziellen Telekommunikationsprovidern zusammen?

Einzelheiten zu den technischen Fähigkeiten des BND können in diesem Zusammenhang nicht öffentlich dargestellt werden. Es wird wiederum auf Fähigkeiten, Methoden und Verfahren der strategischen Fernmeldeaufklärung eingegangen. Gleichzeitig werden operative Details beschrieben, deren Offenlegung negative Folgen für den BND haben könnte. Im Ergebnis würde dadurch die Funktionsfähigkeit der Sicherheitsbehörde und mithin die Sicherheit der Bundesrepublik Deutschland beeinträchtigt. Gleichwohl wird die Bundesregierung nach gründlicher Abwägung dem Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen nachkommen.

Die Informationen werden als „Geheim“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

17. Inwieweit wird für die Überwachung von internationalen Telekommunikationsverbindungen auf die Verbindungsstellen zum Ausland (die sogenannte Auslandskopfüberwachung) zugegriffen?

Die Verpflichtung der Netzbetreiber, technische Vorrichtungen zur Durchführung einer Auslandskopfüberwachung (AKÜ) vorzuhalten, ergibt sich aus § 4 Absatz 2 TKÜV. Eine AKÜ steht grundsätzlich in allen Fällen zur Verfügung, in denen eine entsprechende Beschränkungsmaßnahme angeordnet wurde. Im Übrigen wird auf die Antwort zu Frage 16 verwiesen.

---

* Das Bundeskanzleramt hat die Antwort als „VS – Geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Wie viele „Auslandsköpfe“ werden nach Kenntnis der Bundesregierung bzw. der Regulierungsbehörde für Telekommunikation und Post von welchen Netzbetreibern betrieben?

Derzeit sind der Bundesnetzagentur folgende Unternehmen als Betreiber von sog. Auslandsköpfen bekannt: BT Germany, Cable & Wireless, Colt Telecom GmbH, EPlus, M-net GmbH, Telefonica Germany GmbH, Telekom Deutschland GmbH, TeliaSonera International GmbH, Verizon Deutschland GmbH und Vodafone D2 GmbH.

Die Anzahl der jeweils betriebenen Auslandsköpfe ist hingegen nicht bekannt, da sie für die Frage der Verpflichtung nicht relevant und daher auch nicht Gegenstand der nach § 110 Absatz 1 Satz 1 Nummer 3 TKG und § 19 TKÜV bei der Bundesnetzagentur einzureichenden Unterlagen ist.

18. Gilt das Briefgeheimnis aus Sicht der Bundesregierung auch für elektronische Kommunikation?

    Falls ja, wie wird dann die „vorsorgliche“ Spionage elektronischer Kommunikation gegenüber herkömmlichem Briefverkehr abgegrenzt, der ja nicht anlasslos ausgeforscht wird?

Nein, elektronische Kommunikation unterliegt dem Schutz des Fernmeldegeheimnisses, nicht aber dem Briefgeheimnis. Beide Grundrechte werden von Artikel 10 Absatz 1 des Grundgesetzes geschützt.

19. Welches sind die im PKGr vertretenen unabhängigen Fachleute?

    a) Wer benennt diese Fachleute?

    b) Auf welcher Grundlage wurden diese Fachleute ausgewählt?

Das Verfahren zur Auswahl seiner Mitglieder und die Zusammensetzung des Parlamentarischen Kontrollgremiums ist im Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des PKGrG festgelegt.

20. Kann die Bundesregierung anhand ausgewählter „Treffer“ illustrieren, ob es sich bei der „strategischen Fernmeldeaufklärung“ tatsächlich um ein sinnvolles Instrument zur Feststellung schwerer Straftaten handelt?

Unter den Voraussetzungen des § 7 Absatz 4 G10 hat der BND personenbezogene Daten, die er im Rahmen von G10-Beschränkungsmaßnahmen erlangen konnte, übermittelt. Damit hat er unter Berücksichtigung des in den Übermittlungsvorschriften verkörperten Trennungsgebots zur Abwehr oder Aufklärung schwerer Straftaten einen Beitrag geleistet. Im Übrigen wird auf die Ausführungen zu Frage 14 verwiesen.

Der Aufklärungsansatz wird insbesondere zur Gefahrenbereichsaufklärung im Sinne von § 5 Absatz 1 Satz 3 G10 als notwendig und sinnvoll erachtet.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333